Privacy, Civil Rights, and Civil Liberties Protections: A Key Component of the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)

This document provides an overview of the privacy, civil rights, and civil liberties (P/CRCL) protections that serve as a foundation of the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) and are required in order to participate in the initiative as a fusion center/agency approver. The successful fulfillment of this critical program component is satisfied through the development, adoption, and implementation of an appropriate privacy policy; adherence to the P/CRCL due diligence elements of the NSI; and training of state, local, tribal, territorial (SLTT), federal, and private sector partners.

The NSI is a partnership among SLTT, federal agency, and private sector entities jointly administered by the U.S. Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). It is designed to establish a capacity for appropriately sharing terrorism-related SARs (hereinafter Information Sharing Environment [ISE] SARs [ISE-SARs]) and threat information among the partners to protect our national security. The NSI provides law enforcement and homeland security agencies with another tool to "connect the dots" to combat crime and terrorism by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SARs—also referred to as the SAR process—in a manner that rigorously protects the P/CRCL of Americans.

The SAR process focuses on what law enforcement agencies have been doing for years—gathering information regarding behaviors and incidents associated with crime. The NSI incorporates agencies' individual SAR processes into a nationwide capability and establishes a standardized approach to processing, sharing, analyzing, and using ISE-SAR information, with the goals of detecting and preventing threats to national security, including information associated with domestic and international terrorism. The following briefly describes the key privacy components of the NSI effort.

Suspicious activity is defined in the ISE-SAR Functional Standard (FS) (ISE-SAR FS) as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." The ISE-SAR FS builds upon, consolidates, and standardizes nationwide aspects of those ISE-relevant activities already occurring at the federal, state, and local levels with respect to the processing, sharing, analysis, and use of suspicious activity information. Part B of the ISE-SAR FS also identifies 16 behaviors that a trained analyst or investigator may identify as potential preoperational planning behaviors related to terrorism. These behaviors were identified by subject-matter experts; validated through implementation in the Los Angeles, California, Police Department and the application of ten years of State and Local Anti-Terrorism Training (SLATT®) Program experience; and then adjusted based on input by privacy advocacy representatives. At the completion of this process, in May 2009, the ISE-SAR FS was published, with the entire SAR process anchored on observed behaviors, not race, ethnicity, national origin, or religious affiliation.

NSI Privacy Protection Framework—The NSI requires each fusion center/agency approver to consider privacy throughout the SAR process by fully adopting the following NSI Privacy Protection Framework prior to NSI participation:

- **Privacy policy:** The adoption and implementation of a privacy policy that either meets the ISE Privacy Guidelines (federal agency) or is at least as comprehensive as the Guidelines (fusion centers) and incorporates NSI business processes.
- **ISE-SAR Functional Standard:** The application of the ISE-SAR FS, which reinforces constitutional standards, including the protection of civil liberties guaranteed by the First Amendment and limitations on the use of certain factors—including race, ethnicity, national origin, or religious affiliation—in gathering or collecting, storing, and sharing of personally identifiable information (PII) about individuals. The standard also includes reliability indicators, included as a result of input from privacy advocates. The ISE-SAR FS, through the use of Information Exchange Package Documentation (IEPD), allows the originating agency to include or not include fields that contain PII based upon the agency's rules and policies.
- **Privacy training:** The delivery of privacy training, through which the ISE-SAR FS is effectively communicated to personnel with responsibilities in the ISE-SAR processing/approving arena, ensures the proper application of this standard in the NSI. To expedite privacy policy development and implementation, NSI sites must have access to the services of a trained privacy officer who is available to provide ongoing advice and assistance regarding the protection of P/CRCL. Three levels of training have been developed for the NSI, all of which include an appropriate privacy training focus. The NSI training levels are chief executive, analyst/investigator, and line officer.

Community Outreach—Advocacy groups served an essential role in the shaping of the privacy protection framework and assisted in the development and review of NSI products. The success of the NSI largely depends on the ability to earn and maintain the public's trust. Consequently, NSI sites are encouraged to engage in outreach to members of the public, including P/CRCL advocacy groups and private sector partners, in the course of privacy policy development and implementation. This outreach assists in addressing concerns of citizens and advocates by adopting, maintaining, and communicating appropriate P/CRCL safeguards. A transparent process and collaboration with advocacy groups will reinforce the ongoing commitment to earn and maintain the public trust.

The NSI has developed and participated in the Building Communities of Trust (BCOT) initiative. The role of BCOT is to support local law enforcement agencies and fusion centers as they interact with their various communities to explain the SAR process, the NSI, and the role of federal

agencies, fusion centers, and other NSI participants. Additionally, agencies can use this opportunity to present their privacy policy and outline the safeguards built into the NSI and other information sharing systems.

SAR Vetting Process—A key aspect of the NSI is the SAR vetting process. Before an agency can share SARs in the NSI SAR Data Repository (SDR), two forms of vetting must occur. Supervisors who initially receive a SAR from law enforcement officers, public safety agencies, private sector partners, or citizens must initially review the SAR to determine that it meets the definition of a SAR. If so, it may be submitted for vetting by a trained analyst/investigator at the fusion center or agency. The analyst/investigator undertakes a two-part process to determine whether: (1) the SAR documents one or more of the 16 preoperational behaviors potentially related to terrorism, and (2) considering all the available information (context, facts, and circumstances), there is a potential nexus to terrorism. Throughout the vetting process, P/CRCL are vigilantly and actively protected through the training that analysts and investigators receive and through the system attributes that are a part of the NSI.

System Attributes—In addition to multiple levels of SAR review by trained personnel, there are system attributes that support privacy protections for the gathering, collection, storage, and sharing of SAR information, such as:

- Improved data standards for information sharing using the National Information Exchange Model.
- Leveraging existing secure systems, networks, and resources, such as the Regional Information Sharing Systems®, Law Enforcement Online, the Homeland Security Information Network, the National Criminal Intelligence Resource Center, and the Federal Bureau of Investigation's eGuardian system and Law Enforcement Enterprise Portal (LEEP).
- Built-in design privacy protections, such as user authentication, clearly stated "for official law enforcement use only" warning before system access, and audit logs for capturing search transactions.
- Formatting in accordance with the ISE-SAR FS's IEPD format, which includes the identification of privacy fields.

Compliance Verification—The Global Justice Information Sharing Initiative Criminal Intelligence Coordinating Council developed the *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise* (Compliance Verification document) for the purpose of assisting intelligence and information sharing enterprises in complying with all applicable P/CRCL

protection laws, regulations, and policies while sharing appropriate intelligence and information needed to safeguard America. DHS piloted this document, including the development of a peer-to-peer assessment process, and has encouraged and funded state and major urban area fusion centers to partner with other centers to complete this critical P/CRCL protection assessment.

Future Activity—The NSI is committed to creating a successful information sharing capability to allow SLTT agencies, including state and major urban area fusion centers, and other NSI participating agencies to share SAR information. As the NSI grows and matures, information and systems will be audited. The Compliance Verification document is one version of this audit capability for agencies to use internally.

Since the inception of the NSI, there has been a continued commitment to transparency. SLTT and federal partners met and received input from privacy advocates in the early development stages of the NSI. Law enforcement agencies and fusion centers, through the BCOT program, are meeting with community leaders to engage in dialogue about the NSI. Finally, as updates are made in the NSI and new documents are developed, privacy advocates will continue to be engaged and requested to provide input into these documents.